(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 April 2003 (17.04.2003)

PCT

(10) International Publication Number
WO 03/032618 A1

(51) International Patent Classification⁷: H04M 15/00. H04Q 7/38, H04L 12/28

(21) International Application Number: PCT/SE02/01825

(22) International Filing Date: 8 October 2002 (08.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0103337-2 8 October 2001 (08.10.2001) SE

(71) Applicant *(for all designated States except US)*: SERVICE FACTORY SF AB [SE/SE]; Årstaängsvägen 17, S-117 43 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: PIHLSGÅRD, Johan [SE/SE]; Helenborgsgatan 30, S-117 32 Stockholm (SE). MELLSTRAND, Mats [SE/SE]; Tvärhandsgränd 14, S-393 63 Kalmar (SE).

(74) Agents: DANFELTER, Maria et al.; Albihns Malmö AB, P.O. Box 4289, S-203 14 Malmö (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

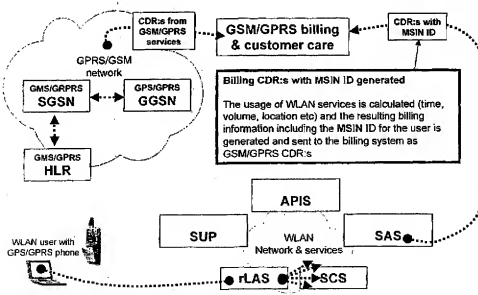
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *of inventorship (Rule 4.17(iv)) for US only*

[Continued on next page]

(54) Title: INTEGRATION OF BILLING BETWEEN CELLULAR AND WLAN NETWORKS



(57) Abstract: According to the illustrated embodiment, the authentication of a cellular network customer in a LAN hotspot area is made possible by a Sign-up server (SUP). The customer enters his cellular phone number (MSISDN) and the SUP contacts the cellular network's HLR via GGSN to get customer identification information (MSIN). SUP creates an account in the system of the LAN network. The generated account details are sent to the users' cellular terminal, e.g. by SMS or e-mail. The usage of LAN services is calculated and the resulting billing information, CDR:s including the MSIN ID, is sent to the cellular network billing system and the customer gets billed by their cellular network operator.

WO 03/032618 A1

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Integration of billing between cellular and WLAN networks

Technical field of the invention

The present invention refers to communication between a data communication network and a cellular network, enabling a cellular network customer to use his customer ID to access services in the data communication network. Especially, the present invention refers to communication between a wireless data communication network, such as WLAN, and a cellular network. The connection between the networks also enables billing information, i.e. consumption of the data communication network service, to be communicated to the cellular network billing system.

Background of the invention

Today, there exist different systems for billing services provided to a customer by means of a data communication network. In the existing systems there is often a need of a separate subscription or agreement between the customer and a service provider, e.g. an operator of the data communication network. Such a subscription can for example be an Internet subscription or the like. However, before concluding an agreement with the customer, the service provider often contacts a credit-rating agency or the like to find out the customer's credit rating. Thus a drawback with the existing system is that the service provider have to contact the credit-rating agency for each new customer, which is both time-consuming and costly for the service provider.

By means of the present invention, the customer can in a much easier way than today get access to and use public data communication networks. This is achieved by letting the customer use his existing relation with a cellular network operator. The billing are simplified - the customer gets one bill for all his network services, and access and authentication is also made easier since it is performed towards the cellular network.

Object of the invention

Objects of the present invention is to enable:

- self-provisioning of WLAN access account for cellular network customers;
- secure transfer of WLAN access credentials to user;
- integration of billing between cellular and WLAN networks, one customer, one billing entity; and
- standard protocol interface between WLAN and the cellular systems.

Summary of the invention

The present invention makes it possible for a customer in a cellular network such as GSM, GPRS, CDMA, UMTS or other standards, to use his or her cellular network customer identity to get authenticated and open an access account in a data communication network, such as a WLAN public access network. The billing relation with the customers' cellular network operator will be used for billing of the WLAN services as well.

Abbreviations and explanations

Below, some of the abbreviations used in this description are explained.

APIS	Application Interface Program Server
CDMA	Code Division Multiple Access
CDR	Call Detail Record
CORBA	Common Object Request Broker Architecture. CORBA is an architecture and specification for creating, distributing, and managing distributed program objects in a network. It allows programs at different locations and developed by different vendors to communicate in a network through an "interface broker".
GGSN	Gateway GPRS Service Node
GPRS	General Packet Radio Services
GSM	Global System for Mobile Communications
HLR	Home Location Register
IMSI	International Mobile Subscriber Identity Number. The IMSI is a unique non-dialable number allocated to each mobile subscriber in the GSM system that identifies the subscriber and his or her subscription within the GSM network. The IMSI resides in the SIM, which is transportable across MSE. The IMSI is made up of three parts (1) the MCC, consisting of three digits, (2) the MNC, consisting of two digits, and (3) the MSIN with up to 10 digits.

BNSDOCID <WO 03032618A1 I >

LCP	Local Connection Point. The term LCP is used to describe a group of access points having a common profile.
LDAP	Lightweight Directory Access Protocol
MCC	Mobile Country Code
MNC	Mobile Network Code
MSE	Mobile Station Equipment. GSM carriers typically order Mobile Station Equipment (MSE), such as GSM phones, from their suppliers, e.g. Ericsson®, Sony®, etc., in large quantities, e.g. 1000 Units. After receiving an order, the equipment supplier will program the ordered MSE SIMs with a range of IMSI numbers.
MSIN	Mobile Subscriber Identity Number
MSISDN	Mobile Subscriber ISDN Number. The MSISDN is the dialable number that callers use to reach a mobile subscriber. Some phones can support multiple MSISDNs – for example, a U.S. based MSISDN and a Canadian based MSISDN. Callers dialing either number will reach the subscriber.
RADIUS	Remote Authentication Dial-In User Service. The RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.
RLAS	Radio Login Access Server. The RLAS is the server to which the access points, e.g. radio antennas and TRX are connected.
SAS	Statistics and Accounting Server
SCS	System Control Server
SDL	System Data Layer
SGSN	Serving GPRS Support Node

SIM	Subscriber Identity Module
SMS	Short Message Service
SUP	Sign-Up Server. The Sign-Up Server is sometimes also abbreviated as SUS.
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VLAS	Virtual LAN Access Server. The VLAS is a generalized access server and firewall which facilitate access, accounting and authorization functions as well as service control and security tasks. VLAS manages user interaction and monitors user communication according to user profile information.
WLAN	Wireless Local Area Network

Brief description of the drawings

Further effects, details and advantages of the system and method according to the present invention are shown by way of example on the accompanying drawings, in which Figs 1 – 6 illustrate chronological steps according to an embodiment of the present invention, realized with a GSM/GPRS cellular network.

Detailed description

The present invention refers to communication between a data communication network and a cellular network, enabling a cellular network customer to use his customer ID to access services in the data communication network. Especially, the present invention refers to communication between a wireless data communication network, such as a WLAN, and a cellular network. The connection between the networks also enables billing information, i.e. consumption of the data communication network service, to be communicated to the cellular network billing system.

An embodiment wherein the cellular system and network is GSM is shown by way of example in the drawings, to which this description refers. The person skilled in the art realizes, however, that the invention is applicable also to other types of cellular systems and networks. Further, the invention will be described

below with reference to a wireless LAN, i.e. to a so-called WLAN, but it should be understood that the invention also is applicable to a LAN.

In the illustrated embodiment, separate terminals, e.g. a mobile phone and a portable computer, are used for communication with the cellular network and the WLAN, respectively. However, in alternative embodiments according to the present invention, these communication functions may be implemented in one and the same terminal device, such as in a Personal Digital Assistant, PDA, or other suitable equipment.

According to the illustrated embodiment, the authentication of a cellular network customer in a WLAN hotspot area, i.e. in an area where a WLAN operator provides a WLAN service, is made possible by a Sign-up server (SUP). The customer enters his cellular phone number (MSISDN) and selects the type of WLAN account he desires. The WLAN account can for example be a permanent account or a time-limited account, e.g. a 24 hours account, but it can also be an account comprising timed-based or volume-based billing etc.

Further, the WLAN operator has an agreement with one or several cellular operators, which agreement allows the WLAN operator to offer services to the cellular operator's customers. Information about allowable services are stored in the HLR of the cellular operator's customer. Thus, when the customer enters his cellular phone number and selects a desired account, the customer also enters the identity of his cellular operator.

The SUP contacts the cellular network's Home Location Register (HLR) via a Gateway GPRS Service Node (GGSN) to verify that the customer is accepted for the selected type of account and to get customer identification information, such as the customer's Mobile Subscriber Identity Number (MSIN). If the customer have entered an incorrect cellular operator or if the WLAN operator is not allowed to provide services to customers, the SUP is prevented from retrieving the customer's MSIN.

The HLR comprises thus a storage structure, such as a database, comprising information about which service or services the user has access to, i.e. if the user has access to e.g. SMS, mobile answering etc.

After the retrieval of the MSIN, the SUP creates an account in the system of the WLAN network, for example in a storage structure connected to an Account Program Interface Server (APIS). The created account comprises the customer identification information (MSIN) and the selected account type. Further, the SUP generates account details, such as username and password, which are stored together with the customer identification number and the selected account type in the APIS. The generated account details, e.g. username and password, are also sent to the users' cellular terminal by for example SMS or e-mail.

The user authenticates to a service or services provided by the WLAN by means of the generated account details, which were sent to him. The usage of WLAN services is calculated based on e.g. the consumed time, volume or location, and the resulting billing information including the MSIN ID is sent to the cellular network billing system as GSM/GPRS Call Detail Record (CDR:s). The customer get billed by the cellular network operator.

The present invention provides also functionality for roaming. In fig. 6 is shown how a WLAN user having a GSM/GPRS home account can access WLAN services from other WLAN operators through roaming. The RADIUS protocol is used for roaming. The billing data is generated and sent together with the user's MSIN ID to the GMS/GPRS billing and customer care system in accordance with the procedure described herein. Further, the rating of the roaming services is controlled by the WLAN user's home operator in the same way as the home operator normally rates cellular calls or other data services.

The present invention hence provides a structured way to communicate between a data communication network, such as a WLAN, and a cellular network, enabling a cellular network customer to use his customer ID to access the services in a WLAN. The connection between the networks also enables billing information, i.e. consumption of the WLAN service, to be communicated to the cellular network billing system.

As a result, the customer can in a much easier way than today get access to and use public WLAN networks. This is achieved by letting the customer use his existing relation with a cellular network operator. The billing are simplified - the customer gets one bill for all his wireless services, and access and authentication is also made easier since it is performed towards the cellular network.

An embodiment of the inventive system comprises a login access point, such as a Radio Login Access Server (RLAS) or a Virtual LAN Access Server (VLAS) to which an end user's computerized device is communicatively connectable or connected. Further, the inventive system comprises a Sign-Up Server (SUP), an Application Program Interface Server (APIS), a Statistics and Accounting Server (SAS) and a System Control Server (SCP). These components of the inventive system will now be more thoroughly described.

Physical Components

The physical components are the units that comprise the physical elements of the inventive system. The units are preferably computerized devices that have been adapted to meet the needs of the system. Depending on the system configuration, certain parameters will vary, others are common to all units.

System software or computer code portions is/are preloaded and includes an operating system that is common to all units. System surveillance is managed by an information manager, e.g. an Information Management (IM) subsystem, which is arranged to transfer control and surveillance data using a network management protocol, such as a Simple Network Management Protocol (SNMP). The IM is implemented throughout the system. To ensure secure terminal access to the system a Secure Shell (SSH) software can be used and communication between nodes or components is protected with encryption software. Time keeping can be performed by means of a time protocol client, such as a Network Time Protocol (NTP) client, which can be implemented in one or several units.

Login access points RLAS/VLAS

The Radio Login Access Server (RLAS) and/or the Virtual LAN Access Server (VLAS) are the parts or nodes of the system that are closest to the end user. The login access points are arranged to function as gathering points for a group of access points in the system. The RLAS and/or VLAS are arranged to handle initial login processes and prevent access to the data communication network until authentication data has been verified by the system, i.e. until the SCS has authenticated the end user. The RLAS/VLAS is further capable to download Local Connection Point (LCP) parameters that further filter who may access the network from a certain access point.

Via a WLAN, a Digital Subscriber Line (DSL) or via some other means, an end user's computerized device is communicatively connectable to the RLAS and/or the VLAS. Independently of the configuration, all Internet traffic by an end user will pass through the RLAS or the VLAS.

An end user can communicate, by means of a laptop, workstation or another suitable computerized device, via a modem with a base station or another public network utility. The base station is in its turn connected to the RLAS/VLAS Ethernet. The initial authentication procedures are handled in the RLAS/VLAS and once the customer credentials have been processed by the system the customer will have access to the service he subscribes to.

The RLAS/VLAS has repeated contact with the SCS and every login attempt goes through the authentication procedure. This involves contacting the SCS comprising the user identification, e.g. usernames and passwords. The RADIUS is an authentication system that can be used to verify end users. The RADIUS client is located in the RLAS/VLAS and the RADIUS server in the SCS.

Accounting data is triggered by an authentication request and these request are recorded in the SCS database before being relayed to the SAS by means of an account manager, such as an Account Management (AM) subsystem. Once an end

user has been authenticated, the RLAS and/or VLAS requests a copy of the product profile data associated with the user in order to build the applicable filter. Further, the SAS is configured to communicate with the RLAS/VLAS via a network manager, such as a SNMP, to retrieve statistical data for example the number of users in session.

The RLAS/VLAS can further be arranged to make a request to find out whether for example branding is indicated in the product profile or not, and if so the specific branding to be used. Branding information can in such cases be included in the LCP parameters. This branding information can be important from a billing point of view since billing information sent to the SAS includes LCP data that can be used to vary the billing models.

Further, a web server is arranged to present the login page to the end user and a mail server is arranged to send a message to a predetermined mail address if the integrity of files is breached.

Sign-up Server SUP

SUP or SUS is the Sign-Up Server used for all on-line registration of customers, SUP also handles the registration and validation of credit card customers. The SUP is communicatively connected to the login access points, i.e. the RLAS and/or the VLAS, and to the APIS. Further, the SUP is arranged to communicate with a cellular network's Home Location Register (HLR) via a Gateway GPRS Service Node (GGSN) to verify that the customer is accepted for the selected type of account and to get customer identification information, such as the customer's Mobile Subscriber Identity Number (MSIN). The SUP can be configured to contact the HLR via for example the SS7 protocol or another protocol used in the public switched telephone system for setting up calls and providing services.

After retrieval of the MSIN, the SUP creates an account in the APIS and generates a customer specific username and password. The generated account details are stored in the APIS together with the MSIN ID for the customer and information about the type of the account. The SUP is further arranged to send the generated username and password to the customer. For example, the SUP can be arranged to send the generated account details by SMS or voice messaging using a voice mail system to the customer's cellular phone, or by an electronic mail to the customers computer. To provide a secure transfer of the generated account details, the SUP can be arranged to use the means for encryption provided for in GSM systems.

When the customer has received his account details, he can authenticate to the WLAN services using his username and password.

Thus, the SUP is configured to handle the initial registration dialogue with a customer, to create accounts and generating account details. However, the SUP can also be arranged to allow a customer to terminate an existing account. Thereby providing a dynamic handling of customers and the belonging accounts.

Further, the SUP can be configured to communicate with a commercial validation system for on-line charging, which validation system is comprised in for example a bank or a credit card institution. This can for example be desirable when the cost for the provided WLAN services are to be withdrawn from the customer's bank account or credit card. Thus, by means of the SUP it is possible for the end user to buy an account and pay for the services by means of the end user's credit card or the like.

Application Program Interface Server APIS

The Application Program Interface Server (APIS) comprises a storage structure, such as a database, for storing configuration data. User's configuration data are created by means of the SUP and stored in the APIS. New configuration data is sent to the APIS and information required by other storage structures in the system is distributed from the storage structure in APIS. In most situations, the configuration data is not static and thus needs to be changed from time to time. Updating of the configuration data can be done from a system console.

A Total Network Application Program Interface (TNAPI) can be comprised in the APIS. The TNAPI is a CORBA based interface, which is used for communication with CABS or an external customer system. Once a time-limited voucher has been activated the SAS acts as the timekeeper and once the time limit has expired a two-way communication is set up between the SAS and the APIS. The SAS initiates the communication by requesting data on the voucher concerned and once the information is received, the SAS will send an account revocation command to the APIS.

Once an administrative user has configured new products and added users, the new information has to be sent to the SCS:s. A configuration manager, such as a Configuration Management (CM) subsystem, is designed to handle the movement of configuration data over the Message Bus (MB). Thus the CM sends information from the APIS to the SCS:s. The CM monitors changes in the APIS database and is activated when they occur.

Communication with a customer administration system is preferably performed via a platform independent architecture, such as the CORBA interface. Such a customer administration system is then configured as a CORBA client, which can access the APIS storage structure.

System Control Server SCS

The System Control Server (SCS) is communicatively connected to the APIS, SAS and RLAS/VLAS servers comprised in the inventive system. The SCS is arranged as a central node for a number of RLAS/VLAS and it is arranged to store a copy of the configuration information that it receives from an APIS, i.e. the passwords and customer information necessary to authenticate end users. Each time an end user logs on to the system a start post is generated. Logging off from the system generates a stop post. These are important from an accounting point of view since these records form the basis of any billing system.

In the event of a positive response to an authentication request, information regarding the end user's unique product profile associated with the end user's account will be retrieved from the storage structure comprised in the SCS. Thus the SCS is arranged to determine what services the end user is entitled to use.

Further, the SCS is configured to send accounting information to the SAS and keeps track of active users. The accounting data is sent to the SAS by the Account Management (AM) subsystem over the message bus. A program in the SCS monitors the local database for changes and is activated when changes are detected. Among these changes are start and stop posts which are forwarded to the SAS.

Remote authentication is handled by RADIUS, which is implemented in the system. The SCS comprises a RADIUS server that handles radius requests originating from end users. Authentication requests identified as belonging to roaming end users are initially handled by leaf SCS:s that relay these to dedicated SCS:s in the system acting as external RADIUS gateways. This is done in order to compile all roaming information in one or two locations making it easier for the individual operator who is then only required to configure external servers on the so-called SCS gateways. It also simplifies matters for roaming partners who are only required to configure one, or at most a few clients and remote servers on their terminals.

Statistics and Accounting Server SAS

The Statistics and Accounting Server (SAS) is arranged to communicate with external billing systems, CABS, APIS, SCS:s and Access Servers. Further, the SAS is arranged to collect billing data, usage data and to revoke time-limited accounts.

The SAS comprises a storage structure, e.g. a database, which comprise accounting data and usage data, programs for processing statistical data and modules for monitoring time-limited accounts. Information, such as start and stop data for each user session, is sent to the SAS from the SCS using the Account management (AM) subsystem. Together with other data, such as the number of

BNSDOCID: <WO_____03032618A1_I_>

bytes sent and/or received, the session duration data is stored in the storage structure of the SAS. The stored information is processed in the SAS before being sent on to an external management system, such as a Netware Management System (NMS), or requested by a Customer Administration and Billing Server (CABS).

The SAS is further arranged to communicate with the APIS to disable accounts that are no longer valid. The task of revoking time-limited accounts is a function handled by the SAS. Time-limited account data is stored in the APIS and the SAS receives start and stop data which it stores in its database. Start and stop data is always accompanied by user ID. The SAS contains a user data reference base. It uses the information stored here to cross check with the APIS as to whether a particular user account exists and what rights it has. If discrepancies are found, a revocation command is sent to the APIS that disables the account.

Usage statistics provided by the SAS, can give the operator valuable information about how the system is utilized. Dimensioning networks is a dynamic process where some areas may need reinforcement and some resources might be underutilized. Usage statistics are retrieved from the RLAS/VLAS by the SAS. The retrieved usage information can for example comprise the number of active sessions in an access point at any time, the number of leases considered active, the number of leases considered free, the total number of IP addresses that can be leased and the ratio in percent of the number active leases and the total number of available leases. This information kind of statistic information can be provided by the SAS and sent to a CABS.

Customer Administration and Billing Server CABS

A Customer Administration and Billing Server (CABS) is a server unit arranged to generate the user interface presented in a system console and arranged to administer all aspects of the system. The CABS specific software handles the input and output data to and from the system console.

The main functions of CABS are to store customer data, present information, such as billing and statistical data, in the system console and communicate with the system through the APIS and the SAS. Further, the CABS can be arranged to deactivate or delete a customer's account.

The CABS retrieves statistical data from the SAS and by means of the system console the administrator can retrieve accounting data and statistics. For example, the operator can search for system usage statistics by requesting a usage report which will include data regarding the total number of users, number of sessions, average session time, average incoming traffic per user and other statistical information.

SDL data can further be altered via the system console. Via for example a CORBA interface between the APIS and CABS, the APIS databases can be read and edited. In this way a system user with the applicable rights can exercise considerable control of the system.

When the system is configured, a super-administrator creates user product profiles, in the number and with the level of authorization required. An end user will thus be associated with a product profile that determines what rights the user is entitled to exercise. In this regard the system is extremely flexible, allowing many variations.

When the administrator add a new Virtual Internet Service Provider (VISP) or changes a user profile via the system console, the new data has to be stored in the APIS database. Thus, the content of the APIS database is changed.

The communication methods employed in CABS are based on the CORBA standard. This makes it possible for pieces of programs called objects to communicate with each other regardless of operating system or computer language. Remote communication and control are easier to implement. Built up with CORBA in mind the Total Network Application Program Interface (TNAPI) is designed to interface with internal and external systems. This means that almost any operator customer and billing system can be used together with the inventive system.

CABS is a complete and independent customer administration and billing system, however operators with existing legacy systems of their own may wish to use the systems they have instead of having dual systems. The TNAPI interface in the APIS is designed for this kind of flexibility. As long as the legacy system supports CORBA it is relatively easy to configure as a CORBA client and in this way exclude CABS from the system.

The graphical presentation of information in the system console is presented as an interactive web page. The web server's primary function is to fetch and display web pages such as the login page on the system console. When the system console is in use, the set of web pages that make up the graphic interface between the user and the system are delivered to the system console by the web server. Most system data is stored in APIS databases apart from some specific end customer data that is stored in the CABS database, such as information about the customer's home address or telephone number.

User Application Server UAS

Embodiments of the inventive system can also be arranged to comprise a User Application Server (UAS). The UAS is a server arranged to provide configuration and generation of user applications. This node is dedicated to end user services like e-mail and the possibility of publishing personal home pages. The

mailboxes and home page repositories required are housed in the UAS. All data access, and the distribution of user accounts, is performed through the SCS.

The UAS is communicatively connected to the APIS for the creation of home directories, which are the repositories for end customer home pages. When new customers are registered and their product profile includes the right to a home page, the APIS will send this information to the database in the UAS.

Further, UAS is also arranged to start an authentication procedure of an end user, since each time an end user wishes read or send mail he/she has to log on to the mail server. This initiates the authentication process using the RADIUS system. The UAS makes contact with the SCS. The RADIUS client in the UAS sends a request to the RADIUS server in the SCS. The RADIUS server queries the LDAP directory in the SCS for authentication and additional data. Security is maintained by the use of symmetrical encryption keys.

Certain product profiles can include notification of new incoming email via SMS. Information about what kind of product profile that matches a certain account is stored on the SCS database. The UAS can be arranged to retrieve this and other accounting data using LDAP.

The system for billing access or usage of a wireless data communication network by intercommunication with a cellular network according to the present invention, comprise means for performing the steps and the functions of the method. Many of the means can be realized as hardware units and most of them are advantageously implemented as computer programs, executing on hardware parts of the arrangement. In particular, a computer program product, for use with a system for billing access or usage of a wireless data communications network by inter-communication with a cellular network, for carrying out an embodiment of the present inventive method and realizing an embodiment of the inventive structure comprises a recording medium and means for performing said method and realizing said structure recorded on the storage medium.

Claims

1. A system for billing access or usage of a data communication network by intercommunication with a cellular network comprising a cellular network billing system, the system comprising:
- a login access point (RLAS, VLAS) configured for communication with an end user's computerized device and for handling an end user's access to said data communication network;
- a sign-up server (SUP) communicatively connected to said login access point (RLAS, VLAS) and configured to verify if said end user is accepted for accessing said data communication network by communicating with said end user's cellular network;
- an application program interface server (APIS) communicatively connected to the sign-up server (SUP);
- a system control server (SCS) communicatively connected to said login access point (RLAS, VLAS), said sign-up server (SUP), and to said application program interface server (APIS), and configured to control the access to said data communication network; and
- a statistics and accounting server (SAS) communicatively connected to said application program interface server (APIS) and to said system control server (SCS), and configured to generate billing information and to send said billing information to said cellular network billing system;

2. The system according to claim 1, wherein said sign-up server (SUP) further is configured to communicate with a Home Location Register (HLR) of said cellular network via a Gateway GPRS Service Node (GGSN).

3. The system according to claim 2, wherein said sign-up server (SUP) further is configured to retrieve an end user identification number from said home location register (HLR) and to authenticate said end user.

4. The system according to claim 3, wherein said end user identification number is said end user's mobile subscriber identity number (MSIN).

5. The system according to claim 4, wherein said sign-up server (SUP) further is configured to create an end user account and to generate end user specific account details.

BNSDOCID <WO_____030328184A1_1_>

6. The system according to claim 5, wherein said sign-up server (SUP) further is configured to create said end user account in said application program interface server (APIS).

7. The system according to claim 5 or 6, wherein said sign-up server (SUP) further is configured to send said end user specific account details to said end user by means of said cellular network.

8. The system according to any the claims 5 – 7, wherein said login access point (RLAS, VLAS) is arranged to receive end user specific account details to verify said end user and to provide access to said data communication network.

9. The system according to any of the claims 5 – 8, wherein said end user specific account details comprises username and password.

10. The system according to any of the preceding claims, wherein said sign-up server (SUP) further is configured to communicate with a commercial validation system for on-line charging of said access.

11. The system according to any of the preceding claims, wherein the data communication network is a wireless data communication network.

12. A method for billing access or usage of a data communication network by intercommunication with a cellular network comprising a cellular network billing system, the method comprising the steps of:
- by means of a computerized device communicating with a login access point (RLAS, VLAS);
- entering an end user's cellular phone number;
- selecting a desired account type;
- communicating with an end user's cellular network to verify if said end user is accepted for accessing said data communication network;
- controlling said access to said data communication network;
- generating billing information related to said end user's access to said data communication network; and
- sending said billing information to said cellular network billing system;

13. The method according to claim 12, further comprising the step of communicating with a Home Location Register (HLR) of said cellular network via a

Gateway GPRS Service Node (GGSN).

14. The method according to claim 13, further comprising the steps of retrieving an end user identification number from said home location register (HLR) and authenticating said end user.

15. The method according to claim 14, further comprising the steps of creating an end user account and generating end user specific account details.

16. The method according to claim 15, further comprising the step of sending said end user specific account details to said end user by means of said cellular network.

17. The method according to claim 15 or 16, wherein said end user specific account details comprises username and password.

18. The method according to any of the claims 15 – 17, further comprising the step of accessing said data communication network by means of said end user specific account details.

19. The method according to any of the claims 12 – 18, further comprising the step of communicating with a commercial validation system for on-line charging of said access.

20. A computer program product for billing access or usage of a data communication network by intercommunication with a cellular network comprising a cellular network billing system, the computer program product comprising means for carrying out the functions or steps of any of the preceding claims.

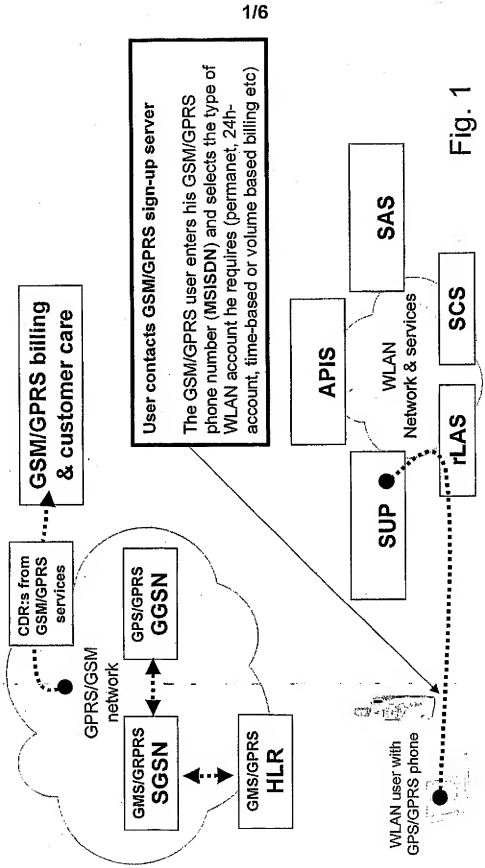


Fig. 1

BNSDOCID: <WO_____03032618A1_I_>

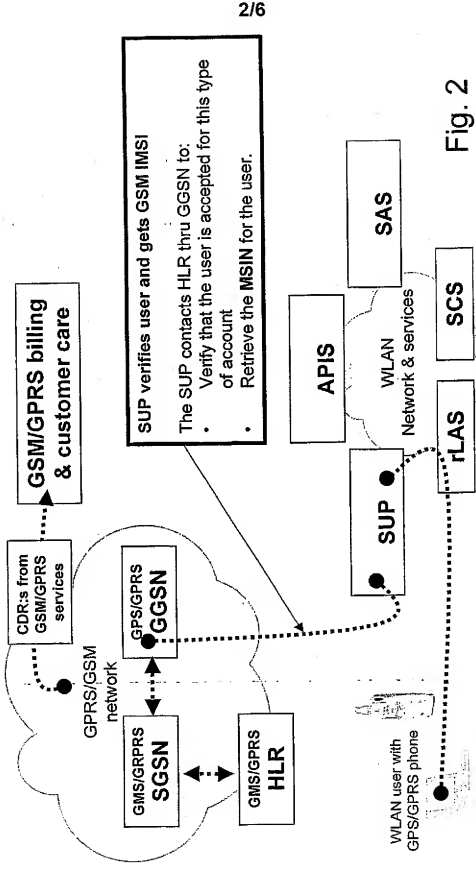


Fig. 2

EMSDOCID <WO 03032618A1_I_>

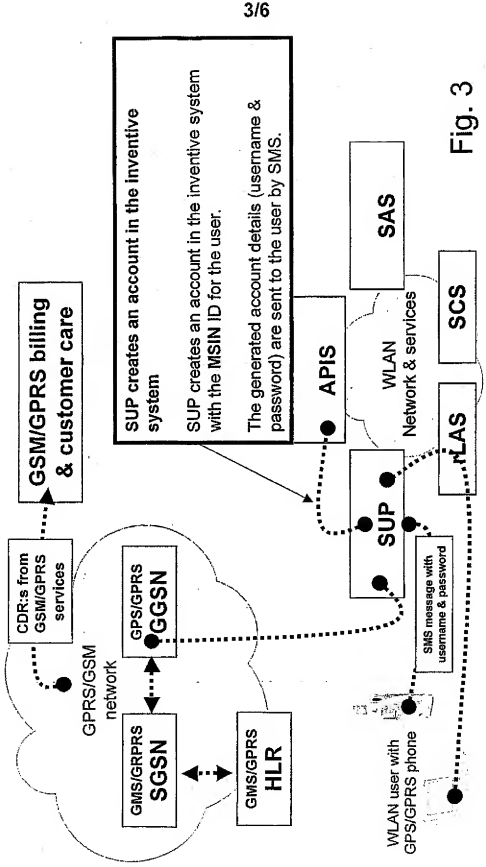

GSM/GPRS billing & customer care
CDR:s from GSM/GPRS services
GPRS/GSM network
GMS/GRPRS SGSN
GPS/GPRS GGSN
GMS/GPRS HLR
WLAN user with GPS/GPRS phone
SMS message with username & password
SUP
APIS
SUP creates an account in the inventive system
SUP creates an account in the inventive system with the MSIN ID for the user.
The generated account details (username & password) are sent to the user by SMS.
WLAN Network & services
SAS
SCS
LAS

Fig. 3

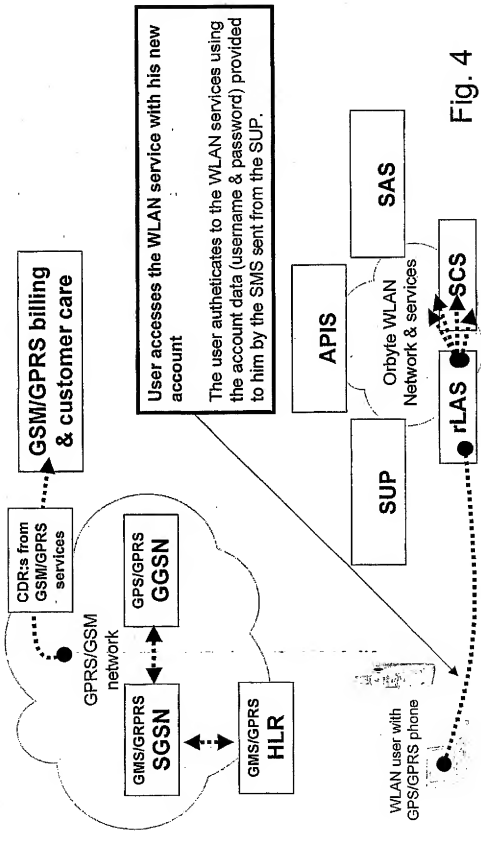

GSM/GPRS billing & customer care
CDR:s from GSM/GPRS services
GPRS/GSM network
GPS/GPRS GGSN
GMS/GRPRS SGSN
GMS/GPRS HLR
WLAN user with GPS/GPRS phone
User accesses the WLAN service with his new account
The user autheticates to the WLAN services using the account data (username & password) provided to him by the SMS sent from the SUP.
SUP
APIS
SAS
Orbyte WLAN Network & services
rLAS
SCS

Fig. 4

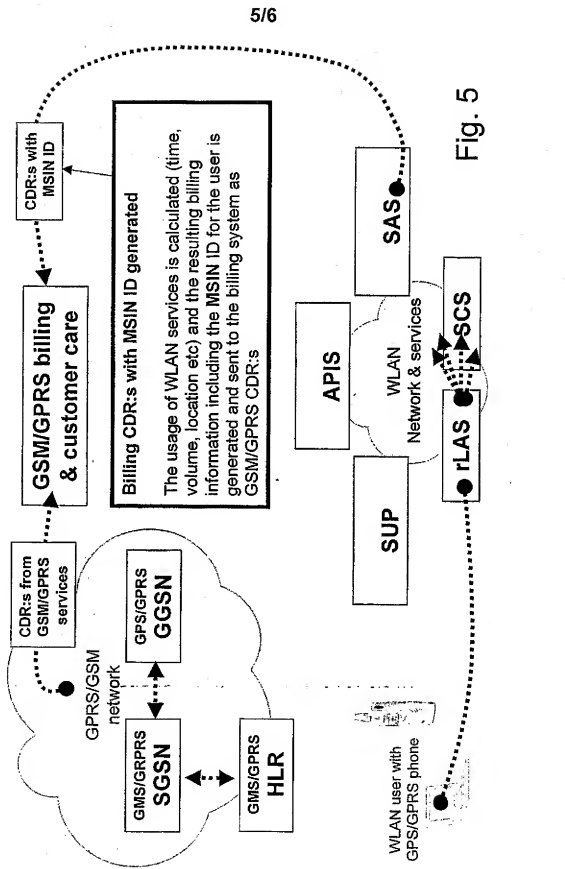

GSM/GPRS billing & customer care
CDR:s with MSIN ID
Billing CDR:s with MSIN ID generated
The usage of WLAN services is calculated (time, volume, location etc) and the resulting billing information including the MSIN ID for the user is generated and sent to the billing system as GSM/GPRS CDR:s
CDR:s from GSM/GPRS services
GPRS/GSM network
GPS/GPRS GGSN
GMS/GRPRS SGSN
GMS/GPRS HLR
WLAN user with GPS/GPRS phone
APIS
SUP
WLAN Network & services
SAS
rLAS
SCS

Fig. 5

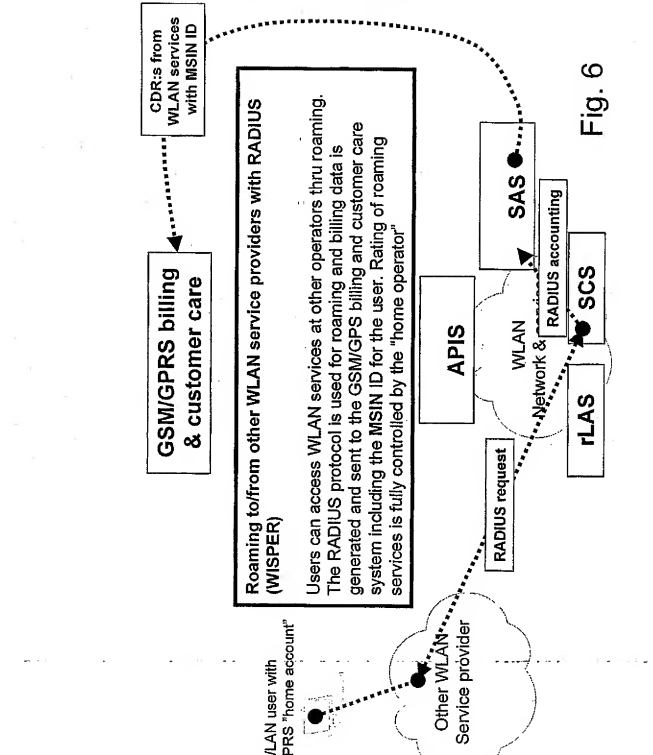


Fig. 6

BNSDOCID <WO_____03032618A1_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 02/01825

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04M 15/00, H04Q 7/38, H04L 12/28
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, H04M, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 0067446 A1 (NOKIA CORPORATION), 9 November 2000 (09.11.00), figure 3B ---	1-4,10-11,20
A	WO 9701920 A1 (TELECOM FINLAND OY), 16 January 1997 (16.01.97), figure 3, claims 1-2, abstract ---	1-20
A	WO 9317516 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 2 Sept 1993 (02.09.93), page 1, line 20 - line 29; page 2, line 10 - line 22, claims 1-3, abstract ---	1-20

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 January 2003	20-01-2003
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Lisbeth Andersson/Els Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

BNSDOCID: <WO_____03032618A1_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 02/01825

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	Databas NPL/EPO, Accession no. XP001107810, ALA-LAURILA J et al, "Wireless Lan Access Network Architecture for Mobile Operators", 2001-11-11, 7110247 Inspec, ISSN 0163-6804, vol. 30 no. 11, pages 82-89, fig. 1-2 --	1-4,10-11,20
P,X	WO 0176297 A1 (NOKIA MOBILE PHONES LTD.), 11 October 2001 (11.10.01), page 6, line 9 - line 23, figure 1, claims 1-3, abstract -- ---	1-4,10-11,20

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

BNSDOCID <WO_____0303281A1_1_>

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SE 02/01825

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0067446 A1	09/11/00	AU 4603100 A	17/11/00
		EP 1175765 A	30/01/02
WO 9701920 A1	16/01/97	EP 0872117 A	21/10/98
		FI 99073 B,C	13/06/97
		FI 953208 A	29/12/96
WO 9317516 A1	02/09/93	AU 666711 B	22/02/96
		AU 3581093 A	13/09/93
		BR 9305924 A	26/08/97
		CA 2130470 A	02/09/93
		CN 1036757 B	17/12/97
		CN 1078339 A	10/11/93
		DE 69326235 D,T	30/12/99
		DK 627150 T	20/03/00
		EP 0592595 A	20/04/94
		EP 0627150 A,B	07/12/94
		SE 0627150 T3	
		ES 2136655 T	01/12/99
		FI 943796 A	18/08/94
		HK 1004249 A	00/00/00
		JP 7506943 T	27/07/95
		KR 273477 B	15/12/00
		MX 9300910 A	01/09/93
		NO 943025 A	16/08/94
		SE 469960 B,C	11/10/93
		SE 9200490 A	20/08/93
		SG 49591 A	15/06/98
		US 5539807 A	23/07/96
WO 0176297 A1	11/10/01	AU 5043901 A	15/10/01
		FI 20000761 D	00/00/00

SEDOCID <WO_____03032618A1_I_>